

REMARKS

Reconsideration and allowance are requested.

Independent claims 1 and 4 stand rejected for anticipation under 35 U.S.C. §102 based on "The PowerPC 604 RISC Microprocessor" (Song). This rejection is respectfully traversed.

To establish that a claim is anticipated, the Examiner must point out where each and every limitation in the claim is found in a single prior art reference. *Scripps Clinic & Research Found. v. Genentec, Inc.*, 927 F.2d 1565 (Fed. Cir. 1991). Every limitation contained in the claims must be present in the reference, and if even one limitation is missing from the reference, then it does not anticipate the claim. *Kloster Speedsteel AB v. Crucible, Inc.*, 793 F.2d 1565 (Fed. Cir. 1986). Song fails to satisfy this rigorous standard.

The independent claims relate to the security of data processing systems and in particular to enhancing their security by masking the processing activity within a data processing apparatus. The inventor recognized that within a system having at least some instructions of an instruction set which may be executed by more than one execution mechanism, the power signature and other characteristics associated with those instructions can be masked by pseudo randomly selecting different execution mechanisms for the instructions. For example, if an instruction may be either executed natively by dedicated hardware or emulated by other software running on the hardware, then this technique pseudo randomly switches between these mechanisms. As well as disguising the power signature associated with the execution of the instruction, the timing of the execution is also markedly altered.

The Examiner alleges that the feature "wherein said execution mechanism selector is configured to be controlled by a pseudo random execution mechanism selecting signal generated by a pseudo random signal generator" is disclosed by Song. Applicant disagrees.

In Song, the execution mechanism selector corresponds to the dispatch buffer described at page 12, left hand column, which selects the execution mechanism based on the data flow and the availability of the resources needed to complete the execution. See page 12, left hand column, second paragraph entitled "Resources available." This dispatch logic in Song is not, and cannot reasonably be viewed as, "a pseudo random execution mechanism selecting signal generated by a pseudo random signal generator." In fact, manipulating the inputs in Song to alter the execution mechanism would likely provide a significant security vulnerability rather than increase security.

A pseudo random signal generator generates a set of values or elements that is statistically random. As will be appreciated by those in this technical field, a pseudo random set of values are not truly random as, for example, that set of values may derived from a known starting point and could be repeated. However, for practical purposes, pseudo random numbers provide necessary values for processes that require randomness, such as creating test signals or for synchronizing sending and receiving devices in a spread spectrum transmission. The generator is "pseudo" random because the generation algorithm can, for example, repeat the sequence, and the numbers are thus not entirely random. One non-limiting example of a pseudo random signal generator in the form of a linear feedback shift register is shown in Figure 7 and is described at page 10, beginning at line 30. A person of ordinary skill in the pseudo random number generation art would not equate "unpredictable events, such as synchronous interrupts and user input" (page 3 of the office action) with a pseudo random signal generator that generates a set of values or elements that is statistically random. Unpredictable events are not pseudo random and could, with appropriate control, have a very regular pattern that would present a significant security vulnerability.

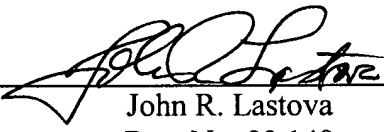
Accordingly, Song's dispatch buffer which selects between the two integer execution units is not controlled by a pseudo random signal generator. The Examiner never identifies any structure in Song that could be reasonably said to be a pseudo random signal generator. Nor does Song's dispatch buffer, responding to "unpredictable events" based on available resources, qualify as pseudo randomly selecting one of the two integer units. The Examiner's interpretation of pseudo random is unreasonable because it is not consistent with the established meaning those of ordinary skill in the art would attribute to pseudo random.

Lacking features recited in the independent claims, the application is in condition for allowance. An early notice to that effect is requested.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: _____


John R. Lastova
Reg. No. 33,149

JRL:maa
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100